IDS in MANETs using Random Walk Detectors

Ashwini Kolekar[1], Harshada Kashid[2], Pooja Chavhan[3] , Priti Ghorpade[4]
Department of Computer Engineering,
Sinhgad College of Engineering,
University of Pune, India.

***Abstract*--This system proposes real time application on Intrusion Detection System (IDS) in Mobile Ad Hoc Networks (MANETs) using Random Walk Detector that aims at overcoming the limitations and weaknesses of the existing IDSs. The proposed IDS incorporates a novel random walk-based IDS architecture as well as a network-layer, specification-based detection engine. The proposed solution does not belong to any of the existing intrusion detection approaches, since it relies on a set of robust, self-contained Random Walk Detectors (RWDs), which may freely move from node to node and randomly traverse a network, while monitoring each visiting node for malicious behaviour. RWDs exhibit a number of benefits including locality, simplicity, low overhead, and robustness to changes in topology. Moreover, the multi-layer, specification-based engine monitors the network layer of the protocol stack, providing an integrated solution capable of detecting the majority of security attacks occurring in MANETs at Network Layer.**

Keywords--Intrusion Detection System, IDS, Mobile ad hoc networks, MANET.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are wireless networks, which operate without the aid of any established infrastructure or centralized authority. MANETs are more prone to attacks than wired network. MANET acts as router in order to handle data traffic network. These characteristics of MANET make it vulnerable to variety of insider attacks. An effective way to identify when an attack occurs in a MANET is the deployment of an Intrusion Detection System (IDS).

On the other hand, the intrusion detectionengines employed in MANETS are classified into three main types: (i) signaturebased, (ii) anomaly-based, and (iii) specificationbased.Signature-based engines rely on a predefined set of patterns (signatures) to identify attacks [1]. The signatures are stored in a database and if the engine matches a monitored activity with a signature, then the activity is marked as malicious. This type of engines fails to detect novel attacks and requires always maintaining a signature database. The anomaly-based engines establish specific models of nodes' behaviors (normal profiles) and mark nodes that deviate from these

profiles as malicious. This type of engines can detect unknown attacks and doesnot require a database. However, it is prone to highrates of false alarms, since any legitimate behaviorthat deviates from normal profiles is also considered as malicious. Finally, specification-based engines rely on a set of constrains or specifications that describe the correct operation of programs or protocols; and monitor the execution of programs/protocols with respect to the defined constraints/specifications. They combine the benefits of both signature and anomaly-based detection, since they: (i) can detect new types of attacks, (ii) do not maintain a database and (iii) do not present high rates of false alarms.

II. THE PROPOSED ARCHITECTURE

The proposed IDS does not require the use of comprehensive detection engines at each network node, like the cooperative architectures, or any static structure like the hierarchical architectures. It consists of several robust RWDs that randomly traverse a network, while monitoring each visiting node for malicious behaviour. The number of RWDs on the network is scalable, in order to cope with changes in the network topology and thus RWDs may replicate or merge.

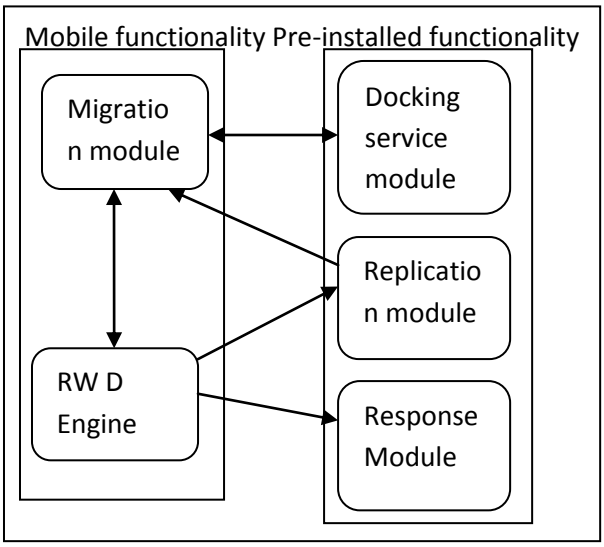


Fig. 1 Layout of RWD

The proposed RWD is divided into five parts as illustrated in in Fig. 1: The migration module and RWD Engineare mobile functionalities. Replication, response, and docking modules are pre-installed in every node

IJERT

1. Migration Module

The migration module isresponsible for the migration process of the RWD toa neighbouring node by establishing a secure communication channel. It is responsible for key generation and key exchange with docking service module using AES and ECDH algorithms respectively.

2. RWD Engine

The multi-layer specification-based detection engine has two main responsibilities: (i) to monitor the migration process of the RWD as mentioned previously; and (ii) to perform detection at the visited node.

$$T_{monitoring} = (T_{min} + T_{critical} + R) \quad (1)$$

*Tmin*denotes the minimum time required by a RWD to detect possible attacks, *Tcritical*is the extra time added because of the criticality/significance of the monitored node, and *R* is a random time added in order to randomize *Tmonitoring*.

3. The replicationmodule

The replication module enables the RWD to be replicated

A generic replication probability is given by (2):

$$P(kRWD) = -(e^{-kRWD}+1)+1 \quad (2)$$

where*kRWD*is the number of neighbours of a node in which the RWD resides at.

4. The response module

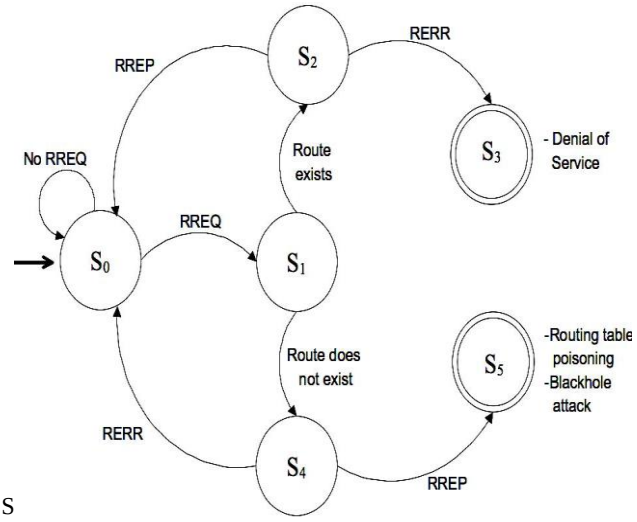
The response module is responsible for notifyingother nodes regarding malicious behaviours detectedand for taking the required defensive action againstthem.

5.The docking service module

The docking service module monitors forincoming RWDs and is responsible for acceptingand establishing a secure connection during themigration process.

III NETWORK LAYER SPECIFICATIONS

In MANETs, connectivity beyond one-hopneighbours is provided by routing protocols, whichrely on the cooperation of all nodes. The mostpopular routing protocols for MANETs are the Ad-hocOn Demand Distance Vector (AODV) and theDynamic Source Routing (DSR).



S

Fig. 2 Network Layer Specification

In Fig. 2, we illustrate a limited set ofspecifications that monitor the AODV routingprotocol, which establishes routes on demand. Toensure its correct operation, the engine supervises allroute control messages at a node. When a noderequires establishing a route to a destination node, itbroadcasts a route request message (RREQ) to all ofits neighbours. Nodes receiving the RREQ store areverse route to the source node and forward the message. When the destination node receives theRREQ, it unicasts a route reply message (RREP)back to the source node. Intermediate nodesreceiving the RREP store the route to the destinationnode in their routing tables. If the route to thedestination node is broken, then a route errormessage (RERR) is transmitted back to the sourcenode.

As presented in Fig. 2, the detection engine awaits for incoming RREQ at the initial state S0. When a RREQ is received, the engine moves to S1 and observes the route validation process performed by the monitored node. If the requested route exists, the engine moves to S2. In this state, the expected behaviour is to reply with a RREP. If this occurs, the route request process is completed and the engine returns to the initial state S0. Otherwise, if the monitored node attempts to reply with a RERR message, the final state S3 is reached, designating a DoS attack, since the node attempts to avoid participation in the routing process. On the other hand, if the requested route does not exist, the engine moves from S1 to state S4. In S4, the legitimate behaviour of the monitored node would be to reply with a RERR message. If this happens, the engine returns to the initial state S0. Otherwise, if the node attempts to transmit a RREP message, the final state S5 is reached, designating a routing table poisoning or blackhole attack. In these attacks, the node misinforms other nodes regarding a nonexisting route. Advertising such a route, the node attracts traffic in order to intercept packets. Then, it drops the packets without forwarding them

IJERT

IVDIFFERENT TYPES OF NETWORK-LAYER ATTACKS

In case of MANET routing is most important thing for proper communication in networksometimes due to wrong attitude of the malicious nodes different types of routing attacks are occurred in network. The network service can be disturbed by an attacker using different techniques.

1. Man In The Middle Attack

The attacker makes independent connections with victims and relays message between them.Entire conversation control by attacker as shown in Fig. 3.

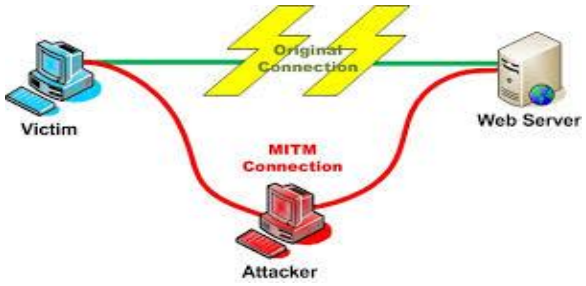
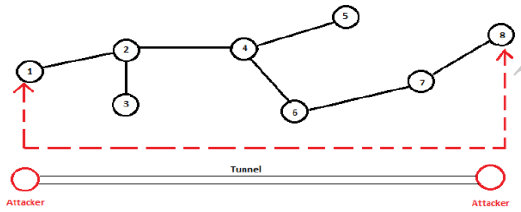


Fig. 3 Man in the middle attack

2.Wormhole Attack

Fig.4 shows Wormhole attack. It issevere attack in which two attackers placed themselves strategically in the network. The attackers keep on hearing the network wireless data.



Wormhole attack

Fig. 4 Wormhole attack

3.Blackhole Attack

Place in network layer where all incoming and outgoing packets are dropped as shown in fig. 5.

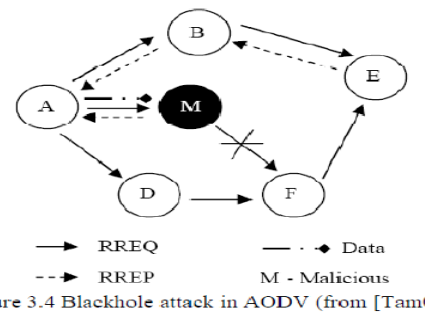


Figure 3.4 Blackhole attack in AODV (from [Tam07])

Fig. 5 Blackhole Attack

4. Routing Table Poisoning

Routing table poisoning causes unwanted or malicious change in routing table in router.It causes severe damage in the network by entering wrong routing table entries in the routing table.

5.DoS Attack

Attempt to make a machine or network resource unavailable to its intended user as shown in fig. 6.

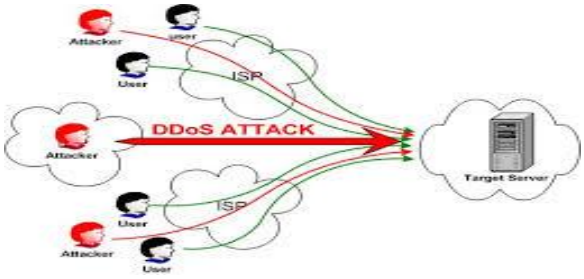


Fig. 6 DoS attack

V MATHEMATICAL MODEL

Let S be the system which consists of

$S=P \cup M$

Where,

$P = \{ P_1, P_2, P_3, \ldots\ldots, P_N \}$

$M = \{ M_1, M_2, M_3, \ldots\ldots, M_Q \}$

N are the number of nodes on which pre-installed functionality is present.

Q are the number of nodes on which mobile functionality is present.

Let P_N be the set of

$P_N = \{K, C, Dm, Rm, Rs \}$

Let mQ be the set of

mQ={ K, C, M, RWDs }

where K= set of symmetric key

C= set of secure channel

Dm= set of docking service module

Rm= set of replication module

Rs= set of Response module

$A.M = \{M_1, M_2, \ldots, M_n\}$

Migration module elects randomly a neighbouring node and generates a symmetric key

$K = \{K_1, K_2, K_3 \ldots, K_n\}$

IJERT

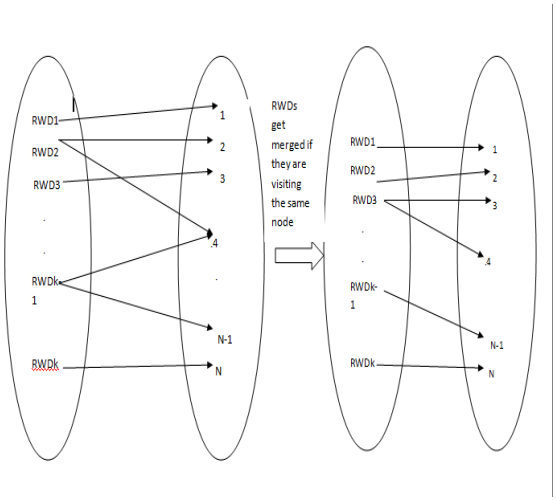
Symmetric key K for migration process

B. C= {C_1, C_2,…..,C_n}

C. RWD= { RWD_1, RWD_2,….., RWD_n}

RWD migrates to the selected node through C.

D.



RWDs get merged if they are visiting the same node.

RWDi → $T_{monitoring}$

Time $T_{monitoring}$for detection engine to detect possible attacks on visited node.

$T_{monitoring}$ = {T_{min}, $T_{critical}$, R}

Where, T_{min}represents minimum time required by RWD to detect possible attacks; $T_{critical}$ represents extra time added; R represents random time to randomize $T_{monitoring}$

Rm = { Rm_1, Rm_2 ,….., Rm_n}
responsible for selecting when RWD will replicate based on probability P.
$P(k_{RWD}) = -(e^{k}{}_{RWD}{}^{+1})+1$
As the number of neighbouring nodes increases , probability for replication increases exponentially.
E. If(Dm && Rs && Rm = = Φ)

Then mark node as malisious else monitor for any malicious acivity.

IJERT

ACKNOWLEDGMENT

We extend our sincere thanks and deep gratitude to our internal guide **Prof. E. Jayanthi**for her valuable advice and guidance without which this project would not have had been possible. We really admire her hard work, dedication and positive attitude. We felt most comfortable under her guidelines while completing project. We are pleased to express our deep sense of gratitude to her.On this occasion we also like to thank Hon' HEAD OF COMPUTER ENGINEERING **Prof. Mr.P.R. FUTANE**. We made the most of his guidelines. We also like to thank Hon' Principalof Sinhgad College of Engineering, Pune**Dr. S. D. LOKHANDE**. We also extend our heartfelt thanks to the non-teaching staff for helping us with everything. Lab attendants also helped us in every manner; they gave the best attention toward our need of software and hardware.Last but not the least we are also thankful to our friends, colleagues and families for their timely help and support.

REFERENCES

1. Christoforos Panos1, Christos Xenakis2 and IoannisStavrakakis, "A novel Intrusion Detection System for MANETs,"Department of Informatics & Telecommunications, University of Athens, PanepistimioupolisIlisia, PC 15784, Athens, Greece.
2. Sen, S., Clark, J. A., "Intrusion Detection in Mobile Ad Hoc Networks, Guide to Wireless Ad HocNetworks", S. Misra, I. Woungang, S.C. Misra (Eds.),Springer, p. 427-454, 2009.
3. Katharine Chang and Kang G. Shin, "Application-layer Intrusion Detection in MANET," The University of Michigan, Ann Arbor, MI 48109-2121 {katchang, kgshin}@eecs.umich.edu.
4. EAACK- A Secure Intrusion Detection System for MANETs. Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE.
5. Li, S., Ephremides, "Covert Channels in Ad-Hoc Wireless Networks," Elsevier Ad Hoc Networks, A, 2009.